UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/506,765	04/14/2005	Yongmao Li	470061.401USPC	8915

500 7590 03/28/2008

SEED INTELLECTUAL PROPERTY LAW GROUP PLLC
701 FIFTH AVE
SUITE 5400
SEATTLE, WA 98104

EXAMINER	
OKEKE, IZUNNA	

ART UNIT	PAPER NUMBER
4193	

MAIL DATE	DELIVERY MODE
03/28/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/506,765	LI ET AL.	
	Examiner	Art Unit	
	Izunna Okeke	4193	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *14 April 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *08 September 2004* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *08/22/2005 and 08/23/2006*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Drawings

1. The drawings are objected to under 37 CFR 1.83(a) because they fail to show "MH12" and "MH21" as described in the specification in Page 5, Line 10 and Page 6, Line 1. Any structural detail that is essential for a proper understanding of the disclosed invention should be shown in the drawing. MPEP § 608.02(d). Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1-5 are rejected under 35 U.S.C. 102(b) as being anticipated by Butler (US-6094487).

a. *Referring to claim 1:*

Regarding claim 1, Butler teaches a method for distributing encryption keys in WLAN, said WLAN having an AP and a plurality of mobile hosts storing identification information, the mobile hosts communicating with the AP through wireless channels, the AP and the external network connecting with the authentication device which authenticates the mobile hosts. The authentication device storing identification information of all mobile hosts (See Butler, Col 1, Line 51-65 teaches a WLAN having a control center as the AP and a plurality of mobile hosts or subscriber units. The control

center functions as both the authentication device and the AP), the method comprising the following steps:

(1) a mobile host sending an authentication request containing identification information to the authentication device for identity authentication (See Butler, Col 4, Line 26-29 teaches a mobile host sending an authentication request to the control center);

(2) the authentication device authenticating the mobile host identification information contained in the authentication request, and if the authentication fails, the authentication device sending an ACCEPT_REJECT message to the mobile host via the AP; and if the authentication succeeds, the authentication device sending key-related information M1 to AP and sending a message comprising ACCESS_ACCEPT information to the mobile host via the AP, and if containing key- related information M2, said message being encrypted (See Butler, Col 6, Line 39-64 teaches the control server sending a reject or denied signal to the host if the authentication fails but if the authentication is successful, the control server sends a message containing the key information. Prior art, XP-001141703, Page 43, Para 8-10 discloses sending of access-accept/reject messages); and

(3) AP obtaining the key from the key-related information M1 sent from the authentication device, and the mobile host obtaining the key from said message sent from the authentication device via the AP (See Butler, Col 3, Line 49-63 teaches the mobile host obtaining the key from the number or message sent from the control device).

b. *Referring to claim 2:*

Regarding claim 2, Butler teaches the method for distributing encryption keys in WLAN of claim 1, wherein said information M1 is the corresponding property information searched by said authentication device according to the identification

information contained in the authentication request, said AP obtains the key through generating it from said property information with a key generation algorithm; whereas said mobile host obtains the key through generating it from property information stored in itself with the same key generation algorithm after said mobile host receives said message comprising ACCESS_ACCEPT information forwarded by AP (See Butler, Butler teaches the control server as both the authentication server and the access point. Col 6, Line 3-38 teaches a second number which is the corresponding property information of the device searched by the authentication agent. Both thee control server and the mobile unit generate the encryption key from this number. See prior art, XP-001141703, Page 43, Para 8-10 discloses an access-accept message included in the transmitted message).

c. *Referring to claim 3:*

Regarding claim 3, Butler teaches the method for distributing encryption keys in WLAN of claim 1, wherein said information M1 is the corresponding property information searched by said authentication device the identification information contained in the authentication request, said AP obtains the key through generating it with a key generation algorithm; said information M2 is the key generated and encrypted by AP with said property information and then sent to said mobile host along with said ACCESS_ACCEPT message, said mobile host obtains the key through decrypting information M2 with said property information (See Butler, Butler teaches the control server as both the authentication server and the access point. Col 6, Line 3-38 teaches a second number which is the corresponding property information of the device searched by the authentication agent. Both thee control server and the mobile unit generate the

encryption key from this number. See prior art, XP-001141703, Page 43, Para 8-10 discloses an access-accept message included in the transmitted message).

d. *Referring to claim 4:*

Regarding claim 4, Butler teaches the method for distributing encryption keys in WLAN of claim 1, wherein said information M1 is the key generated from said property information corresponding to the identification information contained in said authentication request by said authentication device with a key generation algorithm, said mobile host obtains the key through generating it from said property information stored in itself with the same key generation algorithm after receiving said ACCESS_ACCEPT message (See Butler, Col 3, Line 58-65 and Col 4, Line 38—49 teaches the mobile host obtaining the key by generating it from information corresponding to the identification contained in the auth request which is stored in its smart card. Prior art, XP-001141703, Page 43, Para 8-10 discloses an access-accept message included in the transmitted message).

e. *Referring to claim 5:*

Regarding claim 5, the combination of Branigan and Butler teaches the method for distributing encryption keys in WLAN of claim 1, wherein said information M1 and M2 are the key generated from said property information corresponding to the identification information contained in said authentication request by said authentication device with a key generation algorithm, said information M2 is encrypted with said property information and then sent to said mobile host along with said ACCESS_ACCEPT message, said mobile host obtains the key through decrypting said information M2 with the property information stored in itself after receiving said

ACCESS_ACCEPT message (See Butler, Line 15 – 56 teaches a first and second number as keys generated from the property information corresponding to the identification information contained in the request. Prior art, XP-001141703, Page 43, Para 8-10 discloses an access-accept message included in the transmitted message).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claim 10, 15 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Butler (US-6094487), and further in view of Branigan (US-2002/0090089).

a. *Referring to claim 10:*

Regarding claim 10, Butler teaches the method for distributing encryption keys in WLAN of claim 1, Butler does not teach an authentication device is an authentication server installed in said external network. However, Branigan teaches a said authentication device is an authentication server installed in said external network (See Branigan, Para 8 teaches the SB Server as the authentication server installed in a network). Therefore it would have been obvious to one of ordinary skill at the time the invention was made to modify Butler's system to include an authentication server as taught by Branigan for the sole purpose of authenticating the mobile units to the network

b. *Referring to claim 15:*

Regarding claim 15, the combination of Branigan and Butler teaches the method for distributing encryption keys in WLAN of claim 1, wherein said authentication device is a wireless gateway that connects said AP with said external network (See Branigan, Para 8, Line 15-22 teaches the auth device SB server as a wireless gateway that connects the AP with the network).

c. *Referring to claim 20:*

Regarding claim 20, the combination of Branigan and Butler teaches the method for distributing encryption keys in WLAN of claim 1, wherein said authentication device includes said wireless gateway and said authentication server installed in external network (See Branigan, Para 8, and Para 16 teaches the SB Server 102 as the authentication server and also as a wireless gateway installed on the external network).

6. Claim 6-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Butler (US-6094487), and further in view of Mizikovsky (US-6853729)

Mizikovsky system teaches a wireless network comprising a mobile unit and a communication system which comprises an authentication server and an access point or gateway for the wireless mobile unit. For the purpose of the following rejections, the communication system is interpreted as both the authentication server and the access point.

a. *Referring to claim 6:*

Regarding claim 6, Butler teaches the method of distributing encryption keys in WLAN of claim 1. Butler does not teach the steps of (a1) to (e1). However, Mizikovsky teaches the steps of (a1) to (e1) as shown below.

when receiving data packets encrypted with a key sent from the mobile host, said AP updates the key (See Mizikovsky, Col 12, Line 47-54 teaches periodically updating the key) through the following steps of:

(a1) said AP generating a random number and generating a new key from said random number with any key generation algorithm (See Mizikovsky, Col 10, Line 33-49 teaches the system generating a random number and generating a key from the random number);

(b1) said AP adding said random number to a key update message and then sending said message to said mobile host (See Mizikovsky, Col 10, Line 33-50 teaches providing a key update message which includes a random number to the mobile unit);

(c1) when receiving said key update message, said mobile host generating a new key from said random number contained in said key update message with the same key generation algorithm as that in step (a1) (See Mizikovsky, Col 11, Line 10-14 teaches receiving the update key message and generating the new key in a manner used by the system to generate the key);

(d1) said mobile host encrypting the data packets to be sent to AP with said new key and then sending the encrypted data packets to AP, during the encryption process, said mobile host adding an encryption identifier to said data packets and changing the value of said encryption identifier to indicate the communication key has been changed (See Mizikovsky, Col 12, Line 17-54 teaches communications between the unit and the system encrypted with the encryption key and the unit. An encryption identifier, the encryption key is included in the message and the encryption key is changed whenever there is a key update); and

(e1) when receiving the data packets from said mobile host, said AP determines whether

to change the key value of said encryption identifier (See Mizikovsky, Col 12, Line 39-43 teaches between the mobile node and the system and Line 47-50 further teaches the system determining whether to update the key value based on certain criteria).
Therefore it would have been obvious to one of ordinary skill at the time the invention was made to modify Butler's system to include the steps of (a1) to (e1) as taught by Mizikovsky for the purpose of improving the security of the system by updating the key periodically so that any compromised key wont be used on the system for long.

b. *Referring to claim 7:*

Regarding claim 7, the combination of Butler and Mizikovsky teaches the method of claim 1. Branigan and Butler The method for distributing encryption keys in WLAN of claim 1, wherein in order to achieve encryption communication with the new key, when receiving the data packets encrypted with the key sent from said mobile host, said AP updates the key periodically or aperiodically (See Mizikovsky, Col 12, Line 47-54 teaches periodically updating the key) through the following steps of:
(a2) said AP generating a new key in any way and encrypting said new key with the present key (See Mizikovsky, Col 10, Line 50-65 teaches generating a new key which is a cryptographic function a random number and the present key);
(b2) said AP adding the encrypted key to the key update message and then sending said message to said mobile host (See Mizikovsky, Col 10, Line 43-45 teaches providing the unit with the SSD key);
(c2) when receiving said key update message, said mobile host decrypting the new key contained in said key update message with the present key so as to obtain said new key (See Mizikovsky, Col 11, Line 10-14 teaches receiving the update key message and

obtaining the new key in a manner used by the system to generate the key);

(d2) said mobile host encrypting the data packets to be sent to AP with said new key and then sending the encrypted data packets to AP, during the encryption process, said mobile host adding an encryption identifier to said data packets and changing the value of said encryption identifier to indicate the communication key has been changed (See Mizikovsky, Col 12, Line 17-54 teaches communications between the unit and the system encrypted with the encryption key and the unit. An encryption identifier, the encryption key is included in the message and the encryption key is changed whenever there is a key update); and

(e2) when receiving the data packets from said mobile host, said AP determines whether to change the key value of said encryption identifier (See Mizikovsky, Col 12, Line 39-43 teaches between the mobile node and the system and Line 47-50 further teaches the system determining whether to update the key value based on certain criteria).

c. *Referring to claim 8:*

Regarding claim 8, the combination of Butler and Mizikovsky teaches the method for distributing encryption keys in WLAN of claim 1, wherein when receiving the data packets encrypted with the key sent from said mobile host, said AP updates the key periodically or aperiodically (See Mizikovsky, Col 12, Line 47-54 teaches periodically updating the key) through the following steps of:

(a3) said Authentication device generating a random number which is used to generate a new key with the key generation algorithm, and then said authentication device sending said new key to AP, and sending said random number to said mobile host via AP (See Mizikovsky, Col 10, Line 33-66 teaches generating a random number which is used to

generate a new key and sending the random number to the mobile unit);

(b3) said AP sending said key update message to said mobile host after receiving said new key (See Mizikovsky, Col 10, Line 33-50 teaches providing a key update message to the mobile unit);

(c3) when receiving said random number from said authentication device and said key update message from AP, said mobile host generating a new key from said random number with the same key generation algorithm as that in step (a3) (See Mizikovsky, Col 11, Line 10-29 teaches the mobile node generating a new key from the random number with the same key generation algorithm as that in step a3);

(d3) said mobile host encrypting the data packets to be sent to AP with said new key and then sending the encrypted data packets to AP, during the encryption process, said mobile host adding an encryption identifier to said data packets and changing the value of said encryption identifier to indicate the communication key has been changed (See Mizikovsky, Col 12, Line 17-54 teaches communications between the unit and the system encrypted with the encryption key and the unit. An encryption identifier, the encryption key is included in the message and the encryption key is changed whenever there is a key update); and

(e3) when receiving the data packets from said mobile host, said AP determines whether to change the key value of said encryption identifier (See Mizikovsky, Col 12, Line 39-43 teaches between the mobile node and the system and Line 47-50 further teaches the system determining whether to update the key value based on certain criteria).

d. *Referring to claim 9:*

Regarding claim 9, the combination of Butler and Mizikovsky teaches the method for distributing encryption keys in WLAN of claim 1, wherein in order to achieve encryption communication with the new key, when receiving the data packets encrypted with the key sent from said mobile host, said AP updates the key periodically or aperiodically (See Mizikovsky, Col 12, Line 47-54 teaches periodically updating the key) through the following steps of:

(a4) said AP generating a new key in any way and encrypting said new key with the present key, then sending said new key to said AP, whereas sending the encrypted new key to said mobile host via said AP (See Mizikovsky, Col 10, Line 50-65 teaches generating a new key which is a cryptographic function a random number and the present key and providing the key to the mobile host) ;

(b4) after receiving said new key, said AP sending a key update message to said mobile host (See Mizikovsky, Col 11, Line 10-11 teaches the mobile unit receiving a SSD update message sent from the system);

(c4) when receiving the encrypted key from said authentication device and said key update message from said AP, said mobile host decrypting the encrypted key with the present key to obtain a new key (See Mizikovsky, Col 11, Line 10-14 teaches receiving the update key message and obtaining the new key in a manner used by the system to generate the key);

(d4) said mobile host encrypting the data packets to be sent to AP with said new key and then sending the encrypted data packets to AP, during the encryption process, said mobile host adding an encryption identifier to said data packets and changing the value of said

encryption identifier to indicate the communication key has been changed (See Mizikovsky, Col 12, Line 17-54 teaches communications between the unit and the system encrypted with the encryption key and the unit. An encryption identifier, the encryption key is included in the message and the encryption key is changed whenever there is a key update); and

(e4) when receiving the data packets from said mobile host, said AP determines whether to change the key value of said encryption identifier (See Mizikovsky, Col 12, Line 39-43 teaches between the mobile node and the system and Line 47-50 further teaches the system determining whether to update the key value based on certain criteria).

7. Claim 11-14, 16-19 and 21-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Butler (US-6094487) and Mizikovsky (US-6853729), and further in view of Branigan (US-2002/0090089)

f. *Referring to claim 11:*

Regarding claim 11, the combination of Branigan, Butler and Mizikovsky teaches the method for distributing encryption keys in WLAN of claim 6; wherein said authentication device is an authentication server installed in said external network (See Branigan, Para 8 teaches the SB Server as the authentication server installed in a network).

g. *Referring to claim 12:*

Regarding claim 12, the combination of Branigan, Butler and Mizikovsky teaches the method for distributing encryption keys in WLAN of claim 7; wherein said authentication device is an authentication server installed in said external network (See

Branigan, Para 8 teaches the SB Server as the authentication server installed in a network).

h. *Referring to claim 13:*

Regarding claim 13, the combination of Branigan, Butler and Mizikovsky teaches the method for distributing encryption keys in WLAN of claim 8; wherein said authentication device is an authentication server installed in said external network (See Branigan, Para 8 teaches the SB Server as the authentication server installed in a network).

i. *Referring to claim 14:*

Regarding claim 14, the combination of Branigan, Butler and Mizikovsky teaches the method for distributing encryption keys in WLAN of claim 9; wherein said authentication device is an authentication server installed in said external network(See Branigan, Para 8 teaches the SB Server as the authentication server installed in a network).

j. *Referring to claim 16:*

Regarding claim 16, the combination of Branigan, Butler and Mizikovsky teaches the method for distributing encryption keys in WLAN of claim 6; wherein said authentication device is a wireless gateway that connects said AP with said external network (See Branigan, Para 8, Line 15-22 teaches the auth device SB server as a wireless gateway that connects the AP with the network).

k. *Referring to claim 17:*

Regarding claim 17, the combination of Branigan, Butler and Mizikovsky teaches the method for distributing encryption keys in WLAN of claim 7; wherein said

authentication device is a wireless gateway that connects said AP with said external network (See Branigan, Para 8, Line 15-22 teaches the auth device SB server as a wireless gateway that connects the AP with the network).

l. *Referring to claim 18:*

Regarding claim 18, the combination of Branigan, Butler and Mizikovsky teaches the method for distributing encryption keys in WLAN of claim 8; wherein said authentication device is a wireless gateway that connects said AP with said external network (See Branigan, Para 8, Line 15-22 teaches the auth device SB server as a wireless gateway that connects the AP with the network).

m. *Referring to claim 19:*

Regarding claim 19, the combination of Branigan, Butler and Mizikovsky teaches the method for distributing encryption keys in WLAN of claim 9; wherein said authentication device is a wireless gateway that connects said AP with said external network (See Branigan, Para 8, Line 15-22 teaches the auth device SB server as a wireless gateway that connects the AP with the network).

n. *Referring to claim 21:*

Regarding claim 21, the combination of Branigan, Butler and Mizikovsky teaches the method for distributing encryption keys in WLAN of claim 6; wherein said authentication device includes said wireless gateway and said authentication server installed in external network (See Branigan, Para 8, and Para 16 teaches the SB Server 102 as the authentication server and also as a wireless gateway installed on the external network).

o. *Referring to claim 22:*

Regarding claim 22, the combination of Branigan, Butler and Mizikovsky teaches the method for distributing encryption keys in WLAN of claim 7; wherein said authentication device includes said wireless gateway and said authentication server installed in external network (See Branigan, Para 8, and Para 16 teaches the SB Server 102 as the authentication server and also as a wireless gateway installed on the external network).

p. *Referring to claim 23:*

Regarding claim 23, the combination of Branigan, Butler and Mizikovsky teaches the method for distributing encryption keys in WLAN of claim 8; wherein said authentication device includes said wireless gateway and said authentication server installed in external network (See Branigan, Para 8, and Para 16 teaches the SB Server 102 as the authentication server and also as a wireless gateway installed on the external network).

q. *Referring to claim 24:*

Regarding claim 24, the combination of Branigan, Butler and Mizikovsky teaches the method for distributing encryption keys in WLAN of claim 9; wherein said authentication device includes said wireless gateway and said authentication server installed in external network (See Branigan, Para 8, and Para 16 teaches the SB Server 102 as the authentication server and also as a wireless gateway installed on the external network).

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Kimura (US-2001/0048744) discloses an access point device and its authentication method are provided which can dramatically improve a wireless LAN system security level. (See Abstract)

b. Faccin (US-2002/0120844) discloses a method of establishing a connection between a mobile station and a serving domain (See Abstract).

c. Gehrig (US-2003/0048905) discloses a control method, apparatus, and system capable of securely distributing a shared secret network encryption key from a host to a wireless peripheral device. (See Abstract)

d. Ray (US-2003/0112977) discloses communicating data securely within a mobile communications network (See Title)

e. Ekberg (US-7003282) discloses a system and method for authentication in a mobile communications system (See Title)

f. Stenman (US-7028186) discloses the security keys in the mobile terminals and access points of a wireless local area network (WLAN) are created, utilized and managed for a communication session between a mobile terminal and access point. (See Abstract)

g. Engwer (US-7039190) discloses an authentication method features the generation of an initialization vector at a first electronic device and the determination at the first electronic device whether the initialization vector falls within a first group of initialization vectors. (See Abstract)

h. Walker (US-7107051) discloses a method and an apparatus for establishing secured roaming among wireless devices are disclosed. (See Abstract)

i. Weatherspoon (US-7174564) discloses the secure wireless local area network of the present invention includes a single wired network that supports both wired and wireless devices. (See Abstract)

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Izunna Okeke whose telephone number is (571) 270-3854. The examiner can normally be reached on Monday - Friday 7:30 AM - 5:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Long Nguyen can be reached on (571) 272-1753. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

IO

/Taghi T. Arani/
Supervisory Patent Examiner
3/26/2008

/